REMARKS

Claims 21-45 and 48 are pending in the case. The Examiner rejected claims 21-45 and 48 under 35 USC 112, first paragraph. The Examiner also rejected all of the claims over cited prior art. Independent claim 21 has been amended. The following remarks are considered by applicant to overcome each of the Examiner's outstanding rejections. An early Notice of Allowance therefore requested.

The Examiner rejected claims 21-45 and 48 as failing to comply with the written description requirement. In particular, the Examiner contends that since the specification states that the CTA will send both identifiers and status information to a server, which contains preference information on all members and that a link is provided only after the host device is authenticated to the target computer. The applicant has removed this claim language.

The Examiner rejected claims 21-45 and 48 under 35 USC 102 and being anticipated by Rai (US 6,377,982). The applicant has amended claim 21 to clarify the nature of the invention. In particular, claim 21 has been amended to recite that a tunnel is created in the host system through which the client system will access the Internet and that the client is prevented from accessing the resources from the host system. Support for this feature can be found in at least paragraphs [0027-28] of the specification.

The presently claimed invention differs from the known prior art because most of the prior art deals with the creation of a virtual private network wherein the mobile user is trying to access his own secure private network through the public Internet. As the mobile client is solely trying to access their own private secured network through a public resource, there is no concern with accessing the resources of the public Internet. The only security concern is the safety of the communications of the mobile client in reaching his own secured virtual private network. In the present invention, the security interests run both ways – the mobile client wishes to preserve the security of its communication and the host system wishes to allow the mobile client access to his target network through the host system while preserving its own security. This second security concern is never described in the prior art systems that deal with a VPN because it does not exist.

The cited prior art, Rai, falls into this characterization as well. Rai is directed to providing computer users with remote access to the Internet and to private intranets using virtual private network services. Rai describes several different scenarios involving connecting an end

user to a desired target network. In fig. 2, Rai depicts a remote access by an end user through a base station and its router to the Internet. In fig. 3, Rai depicts the same system showing a roaming end user going through a foreign wireless provider then to the home base station. In both scenarios, Rai is only concerned with authenticating the systems and providing the communication path to the Internet (or other desired target network) with security to the communications from the end user. It is not concerned with the security access to the foreign wireless provider and ensuring that the end user cannot access the resources of the foreign wireless provider. Thus, Rai fails to describe the claimed invention which recites that the "client software is prevented from accessing resources outside of said tunnel in said host system." The mere fact that Rai does not describe that the end system does not access the resources of the host system does not mean that it teaches the concept of providing that security interest to the host system. This core concept is important to the present invention because it is a cooperative network which depends on all participants being able to benefit from the relationship and be protected from the relationship. Again, Rai and other prior art references similar to it, do not describe this feature.

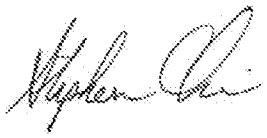
For example, US 6,970,459 (Meier) describes a method of connecting a client system to a home network similar to the virtual private networks described above. While it does describe a L2TP tunnel through the Internet to the home network, it does not describe that a security feature exists that would prevent the client system from accessing the Internet. The security feature is simply about protecting the communication from being accessed through the Internet. This is because there are no security risks involved in traversing the Internet except for the security of the communications of the client system.

In this manner, the teachings of US 6,915,345 (Tummala) does not describe the recited security feature of protecting the host system's resources from the client system. While Tummala does describe a tunnel, the tunnel described therein is solely about protection of the client's systems communication. Again, this type of security is different from the one recited in the claims which protect the host system's resources.

Claims 22-45 and 48 are dependent claims on claim 21 and should be allowable for the same reasons that claim 21 is allowable.

In view of the foregoing, it is respectfully submitted that the claims are in condition for allowance and favorable reconsideration and prompt notice to that affect are earnestly solicited.

Respectfully submitted,



Date: April 18, 2011

Stephen M. Chin
Reg. No. 39,938
Attorney For Applicants
von Simson & Chin LLP
62 William Street – Sixth Floor
New York, New York 10005
ph (212) 514-8645
direct dial (212) 514-8653
fax (212) 514-8648
smc@vsandc.com